

Studierendenrat der Friedrich-Schiller-Universität Jena

Datenschutzempfehlung des
Studierendenrates der FSU-Jena

Beschlossen am: 18.05.2021

Inhaltsverzeichnis

1	Vorwort.....	3
2	Grundlagen für den Datenschutz.....	3
2.1	Gesunder Menschenverstand.....	3
2.2	Richtlinien zur Nutzung sozialer Medien durch den Studierendenrat.....	3
2.3	Telemediengesetz.....	3
2.4	Urheberrechtsgesetz (UrhG).....	3
2.5	Datenschutzgrundverordnung (DSGVO).....	4
2.6	§ 257 HGB (Handelsgesetzbuch) § 147 AO (Abgabenordnung).....	4
2.7	Bundesdatenschutzgesetz (BDSG).....	4
2.8	Medienstaatsvertrag (MStV) besonders §18 Abs. 1 (vormals RStV).....	4
2.9	Kunst-Urheberrechtsgesetz (KunstUrhG) besonders §23.....	4
3	Datensicherheit.....	4
3.1	Redundante Datenspeicherung.....	4
3.2	Schutz vor unbefugtem Zugriff.....	5
4	Webseiten und Social-Media.....	5
4.1	Impressum.....	5
4.2	Datenschutzerklärung.....	7
4.3	Grundsatz der Datensparsamkeit.....	8
4.4	Verwendung von Plugins.....	9
4.5	Hosting der Website.....	10
5	E-Mail-Postfach.....	10
5.1	Hosting der Mail-Adresse.....	10
5.2	Löschung von E-Mails.....	10
5.3	Serienmails und Verteiler.....	10
5.4	Verwendung von Mailprogrammen.....	10
6	Umgang mit analogen und digitalen Daten mit personenbezogenem Inhalt.....	11
6.1	Löschung bzw. Vernichtung von Daten.....	11
6.2	Schutz vor unbefugtem Zugriff.....	12
7	Verwendung fremder Werke (Bild, Ton, Text).....	12
7.1	Beachtung des Urheberrechts.....	12
7.1.a	Unfreie Werke.....	12
7.1.b	Freie Werke.....	13
7.2	Nutzung.....	13
7.3	Beispiele (Werden auf Wunsch erweitert).....	13
8	Anfertigung und Nutzung von Bild- und Tonaufnahmen.....	14
8.1	Wann darf angefertigt und verwendet werden?.....	14
8.1.a	Aufnahme öffentlicher Orte und Gebäude.....	14
8.1.b	Vorlage der Zustimmung (Personen, Orte, Gebäude).....	14
8.1.c	Anfertigung und Nutzung ohne Zustimmung.....	14
8.2	Wann dürfen keine Aufnahmen angefertigt oder verwendet werden?.....	15
9	Nutzung externer Dienste.....	15
9.1	„Frei“ nutzbare Dienste.....	15
9.2	Rechtlich bedenkliche Dienste:.....	15
9.3	Nicht zu verwenden bzw. nur nach StuRa-Beschluss.....	15

1 Vorwort

Die vorliegende Datenschutzempfehlung soll als Orientierung für alle Strukturen des Studierendenrates dienen und eine einfache Übersicht über die wichtigsten Punkte geben. Sie gibt eine Übersicht über die aktuell geltenden Gesetze und die daraus folgenden Aufgaben und Pflichten einer Institution wie dem StuRa.

Es ist zu berücksichtigen, dass diese Empfehlung lediglich von allgemeiner Natur sein kann und von Fall zu Fall individuelle Anpassungen notwendig sein können.

2 Grundlagen für den Datenschutz

2.1 Gesunder Menschenverstand

Der Punkt mag überzogen und ggf. deplatziert erscheinen, angesichts verschiedener Fehlverhalten im Umgang mit dem Datenschutz wird er dennoch angeführt.

Allen Vorhaben sollte ein gewisses Maß an Bedacht zur Seite gestellt werden. Sei dies die Einrichtung einer neuen Website, die Anfertigung von Bild- und Tonaufnahmen oder das Betreiben eines Social-Media-Kanals, jedes solcher Projekte erfordert die Einhaltung gewisser Regelungen und Maßgaben. Da nicht immer jeder alle Punkte berücksichtigen oder im Blick haben kann, sollte lieber einmal mehr als zu wenig nachgefragt werden. Ansprechpartner gibt es hier verschiedene, welche in der eigenen Fakultät, der Uni-Verwaltung oder dem StuRa zu finden sind.

2.2 Richtlinien zur Nutzung sozialer Medien durch den Studierendenrat

<https://www.stura.uni-jena.de/downloads/ordnungen/Medienrichtlinien.pdf>

Durch DSGVO teils veraltet.

2.3 Telemediengesetz

Das TMG regelt verschiedene Angelegenheiten im Zusammenhang mit „[...] elektronischen Informations- und Kommunikationsdienste[n], soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, [...] sind.“

2.4 Urheberrechtsgesetz (UrhG)

Das UrhG regelt Angelegenheiten im Zusammenhang mit Rechten und Pflichten beim Umgang von Werken der Literatur, Wissenschaft und Kunst. Ihm ist immer dann besondere Aufmerksamkeit zu schenken, wenn Werke verwendet werden sollen, an denen eine andere Person Rechte besitzt bzw. besitzen könnte.

2.5 Datenschutzgrundverordnung (DSGVO)

Die DSGVO ist immer dann relevant, wenn Informationen in digitaler Form verarbeitet werden, welche personenbezogene Informationen enthalten.

2.6 § 257 HGB (Handelsgesetzbuch) § 147 AO (Abgabenordnung)

Diese Gesetze sind von Relevanz, sofern die Frage nach der Löschung von Daten gestellt wird, welche im Zusammenhang mit Finanzen stehen.

2.7 Bundesdatenschutzgesetz (BDSG)

Das BDSG regelt Fragen des Datenschutzes auf nationaler Ebene.

2.8 Medienstaatsvertrag (MStV) besonders §18 Abs. 1 (vormals RStV)

Legt unter anderem Pflichten fest, welche Auskünfte Anbieter von Telemedien verfügbar halten müssen. Und das eine Verantwortliche Person zu benennen ist, wenn über ein genutztes Medium „journalistisch-redaktionelle“ Angebote veröffentlicht werden.

2.9 Kunst-Urheberrechtsgesetz (KunstUrhG) besonders §23

Behandelt das Urheberrecht an Werken der bildenden Künste und der Photographie

3 Datensicherheit

Wird über Datensicherheit gesprochen, wird in der Regel die Frage gestellt, ob das nicht das gleiche wie Datenschutz sei. In Gegensatz zum Datenschutz, bei dem die Daten von Personen vor unnötiger, unerwünschter oder unzulässiger Nutzung geschützt werden sollen, ist die Intention der Datensicherheit bestehende Daten (unabhängig ihres Inhaltes) vor Verlust, Veränderung und fremden Zugriff zu sichern.

3.1 Redundante Datenspeicherung

Daten sollten niemals ausschließlich auf einem einzelnen Gerät gespeichert werden, denn nur so kann im Falle eines Gerätedefektes ein Datenverlust vermieden werden. Alle Daten für die eine Mindestspeicherdauer vorgesehen ist, siehe 6.1. , müssen mindestens auf der FSR-Kom-Cloud gespeichert werden oder in den entsprechenden Shared-Laufwerken auf dem File-Server des StuRa. Die Speicherung auf diesen beiden Systemen schließt die lokale Speicherung jedoch nicht aus.

Warum FSR-Kom-Cloud oder File-Server? Die Speicherung der Daten auf diesen beiden Systemen ist einerseits aus Gründen des Datenschutz erforderlich aber auch bezüglich der Datensicherheit. Werden z.B. die Zugangsdaten zu den Speichersystemen verloren, dann kann der Zugang durch die Systemadministratoren des StuRa wiederhergestellt werden. Gehen die Zugangsdaten zu externen Speichersystemen verloren, kann dies einem vollständigen Datenverlust gleichkommen. Die Gründe hierfür sind, dass nicht der StuRa einen Dienstleistungsvertrag mit dem externen Dienst

eingeht, sondern eine Privatperson. Rechtlich sind die Zugänge damit an diese Privatperson gebunden und in aller Regel verweigern die Anbieter die Wiederherstellung der Zugangsdaten, falls der StuRa oder die betroffene StuRa-Struktur eine Anfrage stellt. Vergleichbare Probleme gab und gibt es bereits mit Webseiten, welche durch Privatpersonen angelegt wurden und auf die mittlerweile niemand mehr Zugriff erhält. Alle weiteren Daten, für die keine Mindestspeicherdauer vorgesehen ist, sollten idealerweise ebenfalls auf der Cloud oder dem File-Server gespeichert werden. Müssen aber nicht.

3.2 Schutz vor unbefugtem Zugriff

Nicht öffentliche Daten sind stets vor unbefugtem Zugriff zu schützen. Dies erfolgt im digitalen Bereich etwas durch Passwortschutz oder durch die Verwendung von entsprechenden Nutzungskonten (ebenfalls Passwortgeschützt). Im analogen Fall, werden Daten in einem verschließbaren Schrank etc. gelagert. Hieraus ergibt sich auch die Notwendigkeit, dass ausschließlich Personen von Passwörtern und Zugängen Kenntnis haben dürfen, welche auch berechtigt sind. Beachte Abschnitt 6.2. Auf diese Weise kann sichergestellt werden, dass Daten nicht durch unberechtigte Personen vernichtet, beschädigt, verändert oder zur Kenntnis genommen werden.

4 Webseiten und Social-Media

Der Betrieb einer Website und die Nutzung von Social-Media-Plattformen ist in der gegenwärtigen Zeit ein wichtiges Hilfsmittel zur Verteilung von Informationen und dem Kontaktaufbau mit den Studierenden. Gerade hierbei werden jedoch große Mengen an Informationen verarbeitet. Der richtige Umgang mit der Datenerhebung und Verarbeitung muss daher ein besonderer Augenmerk zugewiesen werden.

4.1 Impressum

Das Impressum ist gemäß § 5 TMG immer verpflichtend, falls die Website oder das Social-Media-Profil nicht ausschließlich privat betrieben wird. Dies betrifft somit alle Angebote, welche durch StuRa-Strukturen angeboten werden.

- Das Impressum muss **jeder Zeit leicht erreichbar und erkennbar** sein.
- Da der StuRa sowohl im Sinne des Datenschutzes als auch des TMG für alle digitalen Auftritte seiner Strukturen verantwortlich ist, ist im allgemeinen eine Verlinkung auf <https://www.stura.uni-jena.de/impressum.php> ausreichend.
- Es sollte zu der Verlinkung oder dem Volltext eine verantwortliche Person im Sinne des §18 Abs. 1 MSvT angegeben werden, welche für die redaktionellen Beiträge verantwortlich ist.

Das Impressum muss in jedem Fall die folgenden Informationen enthalten:

Name der StuRa-Struktur

Vertreten durch:

Studierendenrat der Friedrich-Schiller Universität Jena

Teilkörperschaft öffentlichen Rechts

Carl-Zeiss-Str. 3

07743 Jena

Vertreten durch:

den Vorstand des StuRa der FSU Jena

Kontakt:

Telefon: (03641) 9-400 990

Telefax: (03641) 9-400 993

E-Mail: vorstand@stura.uni-jena.de

Haftungsausschluss:

Haftung für Inhalte

Die Inhalte unserer Seiten wurden mit größter Sorgfalt erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte können wir jedoch keine Gewähr übernehmen. Als Diensteanbieter sind wir gemäß § 7 Abs.1 TMG für eigene Inhalte auf diesen Seiten nach den allgemeinen Gesetzen verantwortlich. Nach §§ 8 bis 10 TMG sind wir als Diensteanbieter jedoch nicht verpflichtet, übermittelte oder gespeicherte fremde Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben hiervon unberührt. Eine diesbezügliche Haftung ist jedoch erst ab dem Zeitpunkt der Kenntnis einer konkreten Rechtsverletzung möglich. Bei Bekanntwerden von entsprechenden Rechtsverletzungen werden wir diese Inhalte umgehend entfernen.

Haftung für Links

Unser Angebot enthält Links zu externen Webseiten Dritter, auf deren Inhalte wir keinen Einfluss haben. Deshalb können wir für diese fremden Inhalte auch keine Gewähr übernehmen. Für die Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich. Die verlinkten Seiten wurden zum Zeitpunkt der Verlinkung auf mögliche Rechtsverstöße überprüft. Rechtswidrige Inhalte waren zum Zeitpunkt der Verlinkung nicht erkennbar. Eine permanente inhaltliche Kontrolle der verlinkten Seiten ist jedoch ohne konkrete Anhaltspunkte einer Rechtsverletzung nicht zumutbar. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Links umgehend entfernen.

Urheberrecht

Die durch die Seitenbetreiber erstellten Inhalte und Werke auf diesen Seiten unterliegen dem deutschen Urheberrecht. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechtes bedürfen der schriftlichen Zustimmung des jeweiligen Autors bzw. Erstellers. Downloads und Kopien dieser Seite sind nur für den privaten, nicht kommerziellen Gebrauch gestattet. Soweit die Inhalte auf dieser Seite nicht vom Betreiber erstellt wurden, werden die Urheberrechte Dritter beachtet. Insbesondere werden Inhalte Dritter als solche gekennzeichnet. Sollten Sie trotzdem auf eine Urheberrechtsverletzung aufmerksam werden, bitten wir um einen entsprechenden Hinweis. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Inhalte umgehend entfernen.

Da das vorgegebene Impressum für die meisten Social-Media-Plattformen zu lang ist, muss eine alternative Lösung gewählt werden. Eine erkennbare Verlinkung auf das Impressum der eigenen Website ist hierfür zulässig. Auf der nachfolgenden Website können verschiedene Vorschläge zur Umsetzung dieser Pflicht nachgelesen werden.

<https://drschwenke.de/impressum-facebook-instagram-google-plus-twitter-youtube-xing-linkedin/>

4.2 Datenschutzerklärung

Wie auch das Impressum, muss auch eine Datenschutzerklärung vorgehalten werden. Die Datenschutzerklärung muss ebenfalls **jeder Zeit leicht erreichbar und erkennbar** sein. Hieraus ergibt sich, dass der Datenschutzerklärung und dem Impressum einen **eigenen Bereich** zugeordnet sein muss und diese **jeder Zeit getrennt erreichbar** sein müssen.

- Eine Verlinkung auf <https://www.stura.uni-jena.de/datenschutz.php> stellt in der Regel die einfachste Lösung dar. **Werden jedoch weitere Dienste auf der eigenen Website genutzt**, welche von der Datenschutzerklärung des StuRa nicht erfasst sind, **muss eine individuelle Erklärung erstellt werden**.

Die Datenschutzerklärung muss folgende Informationen enthalten:

Zwingend:

- *Verantwortlicher:*

*Studierendenschaft der Friedrich-Schiller Universität Jena
Carl-Zeiss-Straße 3
07743 Jena*

*Vertreten durch:
den Vorstand des Studierendenrats der FSU Jena*

*Kontakt Vorstand:
Telefon: (03641) 9-400 991
Telefax: (03641) 9-400 993
E-Mail: vorstand@stura.uni-jena.de*

*Kontakt Datenschutzbeauftragter:
E-Mail: datenschutz@stura.uni-jena.de*

- *Zweck und Rechtsgrundlage der Verarbeitung*
- *Falls Rechtsgrundlage der Art. 6 I f DSGVO ist: Angabe der berechtigten Interessen des Verantwortlichen oder Dritten*
- *Aufklärung über Rechte des Betroffenen (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragung)*
- *Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde*
- *Speicherdauer der Daten (jedenfalls die Kriterien für die Festlegung dieser Dauer)*

Optional bzw. situationsabhängig:

- *Falls eine Einwilligung Rechtsgrundlage ist: Hinweis auf die Möglichkeit des jederzeitigen Widerrufs*
- *Sofern vorhanden: Kontaktdaten des Datenschutzbeauftragten*
- *Bei gesetzlicher oder vertraglicher Pflicht zur Datenerhebung: Aufklärung des Betroffenen über diese Pflicht und die möglichen Folgen einer Nichtbereitstellung*
- *Beim Einsatz automatisierter Entscheidungsfindungen (einschl. Profiling): Aufklärung hierüber, insbesondere die zugrundeliegende Logik, die Tragweite und die angestrebten Auswirkungen für den Betroffenen*

Im Internet stellen verschiedene Rechtsanwaltskanzleien Generatoren für Datenschutzerklärungen zur Verfügung. Diese können für die eigene Website verwendet werden, müssen jedoch ggf. auf individuelle Erfordernisse angepasst werden. Zudem ist bei der Verwendung dieser Generatoren auf die Nutzungsbedingungen der Anbieter zu achten.

4.3 Grundsatz der Datensparsamkeit

Grundsätzlich gilt bei der Erhebung von Daten, die Erhebung muss notwendig und begründet sein, der Grundsatz der Datensparsamkeit zu berücksichtigen ist. **Daher sollte jeder Zeit geprüft werden, ob die zu erhebenden Daten wirklich notwendig sind.** Eine Erhebung von nicht zwingend erforderlichen Daten ist somit zu vermeiden.

Zur Sicherstellung dieses Grundsatzes ist auch darauf zu achten, dass alle Strukturen des Studierendenrates ein Angebot vorhalten müssen, welches eine unkomplizierte und Datensparsame Informationsbeschaffung ermöglicht.

Aus diesem Grundsatz heraus ist zu folgern, dass jede Struktur des Studierendenrates, eine Website anbieten muss, welche die wichtigsten Informationen zu Verfügung stellt. Eine solche Website sollte alle Wichtigen Informationen enthalten, welche für die zu vertretenden Studierenden wichtig sind. Folgende, nicht abschließende, Informationen sollten verfügbar sein:

- Kontaktdaten des eigenen FSR, AK etc.
- Protokolle der öffentlichen Sitzungen, min. jedoch der letzten Sitzung
- Informationen zu Veranstaltungen, sofern sie beworben werden
- wichtige Informationen, sofern sie auch über andere Kanäle veröffentlicht werden

4.4 Verwendung von Plugins

Plugins helfen verschiedene Aufgaben auf einer Website zu erfüllen bzw. zu erleichtern. Hierunter fallen z.B.

- Kalender
- Web-Schriftarten (Web-Fonts)
- Kontaktformulare
- Maps
- Social-Media-Plugins
- etc.

Solche Plugins können durch den Seitenbetreiber selbst betrieben und angewendet werden oder als Dienst eines Drittanbieters eingebunden werden. Da eingebundene Drittanbieterdienste üblicherweise Daten an diese Anbieter übermitteln, ist auf solche Plugins zu verzichten. Eine nicht abschließende Liste mit Plugins, welche nicht verwendet werden sollten ist nachfolgend zu finden.

Nicht zu verwendende Plugins	Alternative
Google-Maps	Open-Street-Maps / freie Aufnahmen von Kartenmaterial (Achtung Anmerkung!)
Plugins zur Reichweitenmessung wie Piwik; Matomo; etc.	Plugins welche nur die Seitenaufrufe zählen, aber keine Nutzerdaten auswerten.
Google-Kalender	OwnCloud-Kalender oder andere Kalender, welche auf der eigenen Website gehostet werden. CMS-Systeme wie Word-Press etc. bieten entsprechende Plugins.
Google-Font, Adobe-Font, etc. Grundsätzlich sind alle Font-Bibliotheken zu meiden, welche während des Webseitenbesuchs eine Verbindung zu den Servern der Anbieter herstellen.	Verwendung von lokalen Schriftarten. Diese können auch aus der Google-Font Bibliothek etc. stammen, müssen aber lokal auf dem eigenen Server vorgehalten werden. ! AGBs der Anbieter beachten !
Social-Media-Plugins, u.a. Verwendung von „Like-Buttons“.	Verwendung von Social-Media-Icons mit manueller Verlinkung. In den meisten CMS-Theme's bereits integriert.
Extern ausgeführte Scripte	Auf dem eigenen Server ausgeführte Scripte

Wichtig! Die Nutzung von Screenshots von Google-Maps etc. ist **i.d.r. verboten**. Ohne eine entsprechende Lizenz zu besitzen, stellt die Nutzung von Screenshots von Google-Maps etc. eine Verletzung des Urheberrechts bzw. der AGB des Anbieters dar.

4.5 Hosting der Website

Websites von Strukturen des Studierendenrates dürfen ausschließlich auf dem Webserver der FSU-Jena oder dem Studierendenrat gehostet werden.

Das Hosten einer Website auf Servern eines anderen Anbieters bedarf explizit der Genehmigung des Vorstandes des Studierendenrates.

5 E-Mail-Postfach

5.1 Hosting der Mail-Adresse

Mailadressen für StuRa-Strukturen dürfen ausschließlich Uni-Mail- oder StuRa-Mail-Adressen sein.

Die Verwendung von Mail-Adressen anderer Anbieter ist aus Gründen des Datenschutzes unzulässig.

5.2 Löschung von E-Mails

Die Speicherung und Löschung von E-Mails stehen im Spannungsverhältnis zwischen der Verpflichtung zur Aufbewahrung von Informationen und der Pflicht zur Löschung.

Siehe Abschnitt 6.1.

5.3 Serienmails und Verteiler

Mails welche an mehrere Adressaten versendet werden sollen, sind **immer** über einen Verteiler zu versenden oder die Adressen der Empfänger sind **immer** in das BCC einzutragen.

5.4 Verwendung von Mailprogrammen

Die Synchronisierung des Mailpostfachs des eigenen FSR, Referates etc. mit dem privaten Endgerät darf nicht erfolgen. Somit darf von Privaten Endgeräten ausschließlich über die Webmailoberfläche zugegriffen werden.

Der Grund hierfür liegt darin begründet, dass bei einer Synchronisierung Daten auf privaten Endgeräten gespeichert würden. Dies würde im Sinne des Datenschutzes eine Weitergabe von personenbezogenen Daten an dritte bedeuten. Weiterhin kann in diesem Fall die Löschung der fraglichen Daten nicht sichergestellt werden.

Bei der Verwendung von **Endgeräten, die Eigentum der Studierendenschaft sind gilt**, falls Mailprogramme wie Thunderbird etc. zum Abruf und Versenden von Mails verwendet werden, müssen diese stets so eingerichtet werden, dass die Daten auf dem Mailserver erhalten bleiben. Daher ist der Mailserver **ausschließlich** über das IMAP Protokoll in das Mailprogramm einzubinden.

6 Umgang mit analogen und digitalen Daten mit personenbezogenem Inhalt

6.1 Löschung bzw. Vernichtung von Daten

Grundsätzlich gilt, ist der Zweck der Speicherung von personenbezogener Daten nicht mehr gegeben, dann sind die Daten oder Dokumente zu löschen oder derart zu anonymisieren, dass ein Rückschluss auf die betroffene Person nicht mehr möglich ist.

Die nachfolgende Tabelle soll eine Übersicht geben, wann welche Daten zu löschen sind.

Gemäß gesetzlicher Mindestspeicherfristen.

Zweck der Speicherung	Dauer der Speicherung
Bücher, Jahresabschlüsse, die Eröffnungsbilanz und die zu ihrem Verständnis erforderlichen Unterlagen, beginnend mit dem Schluss des Kalenderjahres, indem diese angefertigt wurden sind. Gemäß § 147 Abs. 1 Nr. 1, 4 und 4a AO	10 Jahre
Handels- und Geschäftspapiere, wie Rechnungen, Lieferscheine, Kostenvoranschläge und Bewirtungsbelege und sonstige steuerrelevante Unterlagen, beginnend mit Schluss des Kalenderjahres, in dem sie entstanden sind. Gemäß § 147 Abs. 1 Nr. 2, 3 und 5 AO	min 6 Jahre
Bewerbungsunterlagen eines erfolgreichen, folglich eingestellten Bewerbers bis zu drei Jahre nach Schluss des Kalenderjahres, in dem das Arbeitsverhältnis beendet wurde, aufbewahrt werden. Gemäß §§ 195, 199 BGB und § 109 GewO	min 3 Jahre

Gemäß der Beurteilung über die Notwendigkeit der Speicherung

Dokumente/Daten (auch Mails) zum Zwecke der Beantwortung von Beratungsanfragen	Mindestens bis zum Abschluss der Beratung. Empfohlen wird ein Semester. Max. jedoch ein Jahr. *1
Dokumente/Daten (auch Mails) aus interner Kommunikation	Sofern nicht anders bereits erfasst, können diese Daten für die Nachvollziehbarkeit der vergangenen Arbeit max. 4 Jahre gespeichert werden. D.h. die Daten sind nach max. 4 Jahren zu löschen *2. Falls keine Verwendung für die Daten mehr vorliegt, sollten diese Daten bereits früher gelöscht werden.

*1 Die Speicherfrist soll dabei helfen, dass Beratungsanfragen auch im Nachhinein nachvollzogen werden können. Dies kann besonders dann relevant sein, falls sich im Laufe des Semesters Nachfragen durch die beratene Person ergeben.

*2 Sollen solche Daten länger als 4 Jahre gespeichert werden, sind die personenbezogenen Informationen zu anonymisieren.

6.2 Schutz vor unbefugten Zugriff

Alle Daten mit personenbezogenem Inhalt, müssen vor dem unbefugten Zugriff Dritter geschützt werden. Dies bedeutet insbesondere, dass folgende Regeln beachtet werden.

- Beim Verlassen eines PC-Arbeitsplatzes ist der genutzte Account zu sperren um Nutzung durch unbefugte zu vermeiden.
- Passwörter von Webseiten, Mail-Accounts etc. auf welche mehrere Personen zugriff haben, sind bei Bedarf zu ändern, damit nicht-mehr berechnigte Personen keinen Zugriff auf schutzwürdige Daten erhalten können. „Bei Bedarf“ meint immer dann, wenn eine Person mit Zugriffsrechten die Struktur verlässt.
- Unterlagen mit personenbezogen Daten dürfen nicht öffentlich herumliegen.
- Unterlagen mit personenbezogen Daten sind verschlossen zu lagern, sofern unbefugte Personen, ohne Aufsicht, Zutritt zu den Räumlichkeiten haben, in welchen sich die Unterlagen befinden.
- Daten mit personenbezogen Daten dürfen ausschließlich über den Postweg,telefonisch oder über die in 9.1. genannten Kommunikationsdienste übermittelt werden. Andernfalls erfolgt eine Zugänglichmachung gegenüber unberechtigter,externen Dienstleistern.

7 Verwendung fremder Werke (Bild, Ton, Text)

Für die Gestaltung von Webseiten, Flyern, Plakaten, etc. werden verschiedene Designelemente verwendet. Oft stehen diese nicht aus eigener Produktion zur Verfügung und werden daher von externen Autoren verwendet. Hierzu sind verschiedene Punkte bei der Verwendung zu beachten.

7.1 Beachtung des Urheberrechts

Der Autor eines Werkes besitzt in aller Regel das Urheberrecht an diesem Werk. Ausschließlich der Autor oder eine von ihm beauftragte Person entscheidet über die Art und Weise der Verwendung seines Werkes, sofern dies nicht durch Gesetze vorgegeben ist.

Bei der Verwendung eines fremden Werkes ist somit zu jeder Zeit zu prüfen, welchen Bedingungen die Nutzung des Werkes unterliegt.

7.1.a Unfreie Werke

Alle Werke sollten grundsätzlich als unfrei behandelt werden, solange keine Bestätigung für die „Freiheit“ eines Werkes besteht.

Unfreie Werke dürfen entweder gar nicht verwendet werden oder sie benötigen eine individuelle Nutzungserlaubnis des Autors. Eine Erlaubnis wird in aller Regel durch

einen Nutzungsvertrag erteilt und regelt die Art und den Umfang der Nutzung des Werkes. Zudem ist in aller Regel die Erbringung einer Nutzungsgebühr erforderlich.

Wichtig! Ohne die Nutzungserlaubnis des Autors dürfen solche Werke nicht verwendet werden. Bei rechtswidriger oder nicht vertragsgemäßer Nutzung können hohe Vertragsstrafen drohen.

7.1.b Freie Werke

Werke können auf verschiedene Weise „frei“ sein oder werden. Dennoch gelten auch für diese verschiedenen Regelungen bei deren Verwendung.

Wann ist ein Werk frei?

- Der Urheber ist seit 70 Jahren verstorben
- Der Urheber hat sein Werk zur freien Verwendung veröffentlicht. I.d.R. werden solche Werke unter entsprechenden Lizenzen veröffentlicht.

7.2 Nutzung

Werke, auch „freie“ sollten nur verwendet werden, wenn diese entsprechend einer Lizenz veröffentlicht wurden. Dies hängt damit zusammen, dass nur auf diese Weise eine Rechtssicherheit für die Nutzung sichergestellt werden kann.

Die bekannteste Lizenzierung für freie Werke stellt die „Creative Commons“ Lizenz dar. Nicht jede CC-Lizenz erlaubt eine freie Nutzung, weswegen die einzelnen Rechte genau zu prüfen sind. Nähere Informationen können hier nachgelesen werden:

<https://creativecommons.org/licenses/?lang=de>

Für Studierende an einer Hochschule sollte dies zwar außer Frage stehen, dennoch soll darauf hingewiesen werden, dass bei der Verwendung von Werken jeglicher Art der Autor und ggf. die Quelle anzugeben sind.

7.3 Beispiele (Werden auf Wunsch erweitert)

- Veröffentlichung von Skripten: Nur, falls eine Erlaubnis durch den Urheber Vorliegt.
- Veröffentlichung von (Alt-)Klausuren: Nur, falls eine Erlaubnis durch den Urheber vorliegt.
- Veröffentlichung von Mitschriften: Im Falle von 1zu1 Abschriften ist eine Erlaubnis des Dozenten erforderlich. Im Falle von individuellen Zusammenfassungen ist eine Veröffentlichung unter Angabe von Urheber und Quelle zulässig.

8 Anfertigung und Nutzung von Bild- und Tonaufnahmen

Die nachfolgende Übersicht gilt für aufnahmen und Nutzung jeglicher Art von eigens angefertigten Aufnahmen.

8.1 Wann darf angefertigt und verwendet werden?

8.1.a Aufnahme öffentlicher Orte und Gebäude

Ja, ohne weitere Erklärung.

8.1.b Vorlage der Zustimmung (Personen, Orte, Gebäude)

Liegt die Zustimmung der betroffenen Person vor, kann eine Anfertigung und Verwendung nach Maßgabe der Vereinbarung erfolgen. Die Zustimmung sollte zur Wahrung der Rechtssicherheit schriftlich festgehalten werden. **Die Vereinbarung ist durch den StuRa-Vorstand zu bestätigen.**

8.1.c Anfertigung und Nutzung ohne Zustimmung

Die Anfertigung und Verwendung von Aufnahmen ohne die Zustimmung der betroffenen Person ist lediglich zulässig für (§23 KunstUrhG):

- *Bildnisse aus dem Bereiche der Zeitgeschichte;*
- *Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;*
- *Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;*
- *Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.*

Wichtig ist hierbei eine Abwägung zwischen den Rechten der Betroffenen und dem öffentlichen Interesse. Für Aufnahmen in Rahmen universitärer Veranstaltungen sollten damit folgende Aufnahmen zulässig sein:

- Aufnahmen bei öffentlichen Veranstaltungen der Universität (STET, HIT, Fakultätsfest, etc.), sofern die Veranstaltung im Vordergrund steht und nicht eine oder mehrere Personen.
- Aufnahme einer oder mehrerer Personen, wenn dies z.B. eine Auszeichnung einer Person (Lehrpreis etc.) festhält.
- Aufnahme von öffentlichen Veranstaltungen des StuRa, sofern auch hier die Veranstaltung selbst im Zentrum der Aufnahme steht.
-

8.2 Wann dürfen keine Aufnahmen angefertigt oder verwendet werden?

- Keine der in Punkt 8.1 genannten Bedingungen ist erfüllt
- Andere, noch nicht berücksichtigte Regelungen verbieten die Anfertigung oder Verwendungen
- **Nicht erlaubt** sind Aufnahmen und deren Verwendung, von nicht öffentlichen Veranstaltungen. Es gilt jedoch eine Ausnahme, falls alle betroffenen Personen der Aufnahme und Verwendung zustimmen. Hier runter fallen u.a. (Klausurtagungen, KlaVoWo, etc.)

9 Nutzung externer Dienste

Die Nutzung externer Dienste, unterliegt dem generellen Regelungen zum Abschluss von Verträgen. Da nahezu alle externen Dienste einer Nutzungsordnung bzw. AGB unterliegen, muss diesen vor Nutzung zugestimmt werden. Diese Zustimmung darf nach geltenden Recht jedoch nur durch den Vorstand des StuRa gegeben werden oder auf Grund von Beschlüssen des StuRa.

9.1 „Frei“ nutzbare Dienste

- BigBlueButten (StuRa und Universität)
- Webserver (StuRa und Universität)
- Mailserver (StuRa und Universität)
- Clouddienste (StuRa und Universität)
- Matrix-Server (StuRa)

9.2 Rechtlich bedenkliche Dienste:

Auf die Verwendung dieser Dienste sollte verzichtet werden.

- Alle Video-Konferenz Dienste via FSU-Account, welche die Uni nicht selbst betreibt.
 - Zoom, MS-Teams, Cisco-Webex, etc.
- Alle weiteren Dienste, für welche die FSU zwar Lizenzen besitzt, die Dienste jedoch nicht selbst betreibt.

9.3 Nicht zu verwenden bzw. nur nach StuRa-Beschluss

- Social-Media-Plattformen. (Die Nutzung von Facebook ist durch StuRa-Beschluss für FSRe und Campusmedien gestattet)
- Alle Video-Konferenz Dienste, welche noch nicht genannt wurden d.h. alle Dienste, für die ein separater Nutzungsvertrag eingegangen bzw. (privater) Account erstellt werden muss. Z.B.: Skype, Mumble, Teamspeak, Discord

- Alle Dienste von Google. Z.B.: Google-Maps, Google-Kalender, Google-Font-Plugin, Google-Mail, Google-Forms, YouTube ... (Die Nutzung von YouTube ist für Campusmedien über StuRa-Beschluss gestattet)

Neben den hier genannten Diensten sind alle weiteren Dienste erst nach Beschluss durch den StuRa zu verwenden, sofern sie nicht in 9.1. bzw. 9.2. aufgeführt sind.